Creation of DLP Security Policies

He enfocado este proyecto de **Prevención de Pérdida de Datos (DLP)** utilizando **tecnologías Microsoft** debido a mi experiencia previa en el uso e implementación de soluciones como **Microsoft Intune, Microsoft Purview (antes Information Protection), Defender for Endpoint y Azure Active Directory**.

Durante mi trayectoria profesional he trabajado directamente con estas herramientas en entornos empresariales, lo que me ha permitido adquirir un conocimiento práctico sobre su integración, gestión y potencial para proteger datos confidenciales. Gracias a esta experiencia, considero que Microsoft ofrece una solución robusta y escalable para implementar políticas DLP efectivas, especialmente dentro de organizaciones que ya operan con Microsoft 365.

Introducción al Data Loss Prevention (DLP)

El *Data Loss Prevention* (DLP), o Prevención de Pérdida de Datos, es un conjunto de estrategias y herramientas diseñadas para detectar y prevenir la exposición, transmisión o utilización no autorizada de información sensible dentro de una organización. Su objetivo principal es proteger los datos críticos, ya sean financieros, personales, estratégicos o legales, y evitar que sean comprometidos por errores humanos, amenazas internas o ciberataques.

La importancia del DLP en una organización radica en su capacidad para:

- **Cumplir con normativas** de protección de datos (como GDPR, HIPAA, etc.).
- **Proteger la propiedad intelectual** y secretos industriales.
- **Preservar la reputación empresarial** al evitar filtraciones públicas de información.
- **Mitigar riesgos financieros y legales** derivados de la pérdida de datos confidenciales.

Un programa de DLP robusto no solo protege la información crítica de una organización, sino que también crea una cultura de seguridad en todos los niveles. Con políticas claras, tecnología adecuada y un personal informado, se reduce significativamente el riesgo de fugas de información y se fortalece la postura de ciberseguridad corporativa.

Implementación de Políticas DLP en OneDrive usando Intune, Azure AD y Microsoft Defender

Contexto: Empresa de Consultoría Financiera

Una empresa mediana de servicios financieros con 120 empleados utiliza **OneDrive for Business** (parte de Microsoft 365) como su principal sistema de almacenamiento en la nube. Los empleados gestionan datos de clientes, documentos fiscales y contratos legales, por lo tanto, se requieren medidas de seguridad estrictas para proteger esta información sensible.

Objetivo

Implementar una política de Prevención de Pérdida de Datos (DLP) basada en el **Principio del Menor Privilegio**, exclusivamente usando las siguientes tecnologías Microsoft:

- **Microsoft Intune**: Gestión de dispositivos y cumplimiento.
- **Azure Active Directory (Azure AD)**: Control de identidad y acceso.
- **Microsoft Defender for Endpoint / Cloud Apps**: Protección en tiempo real y control de actividades.
- **Microsoft Purview**: Clasificación y etiquetado de datos sensibles.

Políticas de Seguridad Implementadas

1. Clasificación de Datos con Microsoft Purview

Se definieron las siguientes etiquetas automáticas:

Etiqueta	Descripción	Acciones Automáticas
Público	Información general de bajo riesgo	Compartible con usuarios internos
Interno	Uso restringido dentro de la empresa	No se permite compartir externamente
Confidencial	Datos fiscales, bancarios, clientes	Cifrado automático, acceso limitado, monitoreo activo

Microsoft Purview detecta datos como números IBAN, CIF/NIF, nombres de clientes y palabras clave como "contrato" o "declaración", y asigna etiquetas automáticamente.

---

2. Acceso Controlado con Azure AD y el Principio del Menor Privilegio

Políticas de Azure AD:

- **Grupos de Seguridad Dinámicos**: empleados se agrupan automáticamente según su puesto (por ejemplo: “Finanzas”, “Legal”, “Comercial”).
- **Políticas de Acceso Condicional**:
    - MFA obligatorio para todos los accesos a OneDrive.
    - Bloqueo de acceso desde ubicaciones no aprobadas.
    - Solo dispositivos registrados y conformes pueden acceder a documentos **Confidenciales**.

Ejemplo:

Un empleado del departamento de Marketing no puede acceder a documentos etiquetados como “Confidencial - Finanzas”, ni siquiera si recibe el enlace.

---

3. Gestión de Dispositivos con Microsoft Intune

- **Cifrado Obligatorio con BitLocker** en todos los portátiles gestionados.
- **Control de USB**: Intune bloquea el uso de dispositivos extraíbles salvo autorización explícita del administrador.
- **Política de cumplimiento**: si un dispositivo pierde el cifrado o es jailbreak/root, se revoca el acceso automáticamente a OneDrive y apps de Microsoft 365.

Protección Adicional:

- Aplicación de política de “No copiar/pegar” y bloqueo de impresión para datos etiquetados como **Confidenciales** dentro de aplicaciones móviles de Office 365.

---

4. Monitoreo y Detección de Riesgos con Microsoft Defender

- **Microsoft Defender for Endpoint** supervisa:
    - Actividades anómalas (descargas masivas, exfiltración sospechosa).
    - Uso de herramientas no autorizadas (por ejemplo, intento de cargar archivos confidenciales a servicios como Dropbox).
- **Microsoft Defender for Cloud Apps**:
    - Detecta sesiones en OneDrive que provienen de ubicaciones o dispositivos no confiables.

- Bloquea automáticamente movimientos no autorizados de archivos etiquetados.

Alertas configuradas:

- Más de 50 archivos confidenciales descargados en una hora.
- Intento de compartir archivo clasificado con usuario externo.
- Acceso desde dispositivo no conforme.

Resultados

- Reducción en intentos de compartir información confidencial fuera de la organización.
- 100% de los dispositivos críticos cifrados y conformes con las políticas DLP.
- Auditorías semanales generadas automáticamente para revisiones por parte del CISO.

Conclusión

El uso coordinado de **Azure AD, Microsoft Intune, Microsoft Defender y Purview** permitió establecer un entorno de seguridad robusto, centralizado y automatizado, aplicando el principio del menor privilegio en todos los niveles: usuarios, dispositivos y datos. La empresa ahora opera con mayor confianza en la seguridad de su información crítica, sin sacrificar productividad.
